IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

| | | |
|---|---|---|
| IN RE SEARCH WARRANT MAG. NO. 16-4116 (MAH) TO GOOGLE, INC. | ) | Hon. Madeline Cox Arleo |
| | ) | Docket No. 2:17-cv-5847 (MCA) |
| | ) | (Related to Mag. No. 16-4116) |

MEMORANDUM OF LAW OF THE GOVERNMENT IN RESPONSE TO GOOGLE INC.'S OBJECTIONS TO MAGISTRATE ORDER

WILLIAM E. FITZPATRICK
Acting United States Attorney
970 Broad Street
Newark, New Jersey 07102
(973) 645-2700

On the Memorandum:

L. Judson Welle
Bruce P. Keller
Assistant United States Attorneys

Andrew S. Pak
Trial Attorney
Computer Crimes & Intellectual Property Section
United States Department of Justice

## TABLE OF CONTENTS

**Page**

TABLE OF AUTHORITIES ..... iii

PRELIMINARY STATEMENT ..... 1

BACKGROUND ..... 3

I. The Stored Communications Act. ..... 3

II. Judge Hammer's Decision. ..... 5

ARGUMENT ..... 9

I. Requiring Google To Produce Information In Its Possession, Custody, Or Control Is A Domestic Application Of The SCA's Warrant Provisions. ..... 9

A. The "Focus" Of The SCA's Warrant Provisions Is Required "Disclosure." ..... 10

B. Even Under Google's Privacy-Centric Reading Of Section 2703, The SCA Operates Domestically. ..... 12

II The SCA Provides Courts With Power *In Personam* To Require U.S. Providers To Produce Information In Their Custody Or Control, Regardless Of The Location Of The Information. ..... 16

A. The SCA Grants Courts Power *In Personam* To Compel Providers To Produce Information. ..... 17

B. The SCA Allows Courts To Compel U.S. Providers To Produce Information Within Their Custody Or Control Irrespective Of Where The Data Is Located. ..... 19

C. Congress's Use Of The Term "Warrant" Was Meant To Import The Probable Cause Standard, Not To Impose A Territorial Limit. ..... 22

D. Google's Purported "Caretaker" Status Is Irrelevant. ..... 26

E. Google's Analogy To The Wiretap Act Is Unavailing. ..... 29

III Google Raises Unsupported And Unwarranted Concerns Regarding International Comity. ..... 31

CONCLUSION ..... 35

## TABLE OF AUTHORITIES

**Cases** **Page(s)**

*Anschuetz & Co., GmbH. v. Mississippi River Bridge Auth.*,
483 U.S. 1002 (1987) ..... 21

*Blackmer v. United States*,
284 U.S. 421 (1931) ..... 21

*EEOC v. Arabian American Oil Co.*,
499 U.S. 244 (1991) ..... 32

*Exch. Comm'n v. Minas De Artemisa, S. A.*,
150 F.2d 215 (9th Cir. 1945) ..... 21

*Fisher v. United States*,
425 U.S. 391 (1976) ..... 27

*Gerling Int'l Ins. Co. v. CIR*,
839 F.2d 131 (3d Cir. 1988) ..... 20

*In re Search of Info. Associated with Accounts Identified as [redacted]@gmail.com*,
No. 2:16-MJ-02197-DUTY-1, 2017 WL 3263351 (C.D. Cal. July 13, 2017) ... 2

*In re Search of Info. Associated with [redacted]@gmail.com that is Stored at Premises Controlled by Google, Inc.*,
No. 16-MJ-00757 (BAH), 2017 WL 3445634 (D.D.C. July 31, 2017)
..... 2, 11, 13, 14

*In re Search Warrant No. 16-960-M-01 to Google*,
232 F. Supp. 3d 708 (E.D. Pa. Feb. 3, 2017) aff'd, 2017 WL 3535037 (E.D. Pa. Aug. 17, 2017) ..... 2, 32

*In re Two Email Accounts Stored at Google Inc.*,
No. 17-MJ-1235, 2017 WL 706307 (E.D. Wisc. Feb. 21, 2017) ..... 2, 22

*In the Matter of the Search of Content Stored at Premises Controlled by Google Inc. & as Further Described in Attachment A*,
No. 16-MC-80263-RS, 2017 WL 3478809 (N.D. Cal. Aug. 14, 2017) ..... 2

*Hale v. Henkel*,
201 U.S. 43 (1906) ..... 21, 27

*Hay Group, Inc. v. E.B.S. Acquisition Corp.*,
360 F.3d 404 (3d Cir. 2004) ..... 19, 20

*In re Anschuetz & Co., GmbH*,
754 F.2d 602 (5th Cir. 1985) ..... 20

*In re Sealed Case*,
832 F.2d 1268 (D.C. Cir. 1987), *abrogated on other grounds by Braswell v. United States*, 487 U.S. 99 (1988) ..... 21

*In re Search Warrant to Google, Inc.*,
No. 16-4116-MAH, 2017 WL 2985391 (D.N.J. July 10, 2017) ..... passim

*In the Matter of a Warrant for All Content & Other Info. Associated with the E-mail Account xxxxxxx gmail.com Maintained at Premises Controlled By Google, Inc.*,
33 F. Supp. 3d 386 (S.D.N.Y. 2014), as amended (Aug. 7, 2014) ..... 13

*Kiobel v. Royal Dutch Petroleum Co.*,
133 S. Ct. 1659 (2013) ..... 9, 32

*Kirtsaeng v. John Wiley & Sons, Inc.*,
133 S. Ct. 1351 (2013) ..... 22

*Marc Rich & Co. v. United States*,
707 F.2d 663 (2d Cir. 1983) ..... 20

*Matter of Search of Content that is Stored at Premises Controlled by Google,*
No. 16-MC-80263-LB, 2017 WL 1487625 (N.D. Cal. Apr. 25, 2017) ..... 2, 18

*Matter of Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.,*
13 F. Supp. 3d 157 (D.D.C. 2014) ..... 13

*Matter of Search of Info. Associated with [Redacted]@gmail.com That is Stored at Premises Controlled by Google, Inc.,*
No. 16-MJ-757 (GMH), 2017 WL 2480752 (D.D.C. June 2, 2017) ..... 2, 16

*Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*,
829 F.3d 197 (2d Cir. 2016) ..... 1, 10, 16, 23

*Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.,*
855 F.3d 53 (2d Cir. 2017) ..... passim

*Morrison v. National Australia Bank Ltd.*,
561 U.S. 247 (2010) ..... 7, 9, 10, 11

*In re Two email accounts stored at Google, Inc.*,
No. 17-MJ-1235, 2017 WL 2838156 (E.D. Wisc. June 30, 2017) ..... 2, 17

*Republic of the Philippines v. Marcos*,
862 F.2d 1355 (9th Cir. 1988) ..... 19

*RJR Nabisco, Inc. v. European Community*,
136 S. Ct. 2090 (2016) ..... passim

*Samantar v. Yousuf*,
560 U.S. 305 (2010) ..... 22

*Reinsurance Co. of Am. v. Administratia Asigurarilor de Stat (Admin. of State Ins.)*,
902 F.2d 1275 (7th Cir. 1990) ..... 20, 32

*State of New Jersey v. City of New York*,
283 U.S. 473 (1931) ..... 19

*Steele v. Bulova Watch Co., Inc.*,
73 S. Ct. 252 (1952) ..... 19

*United States v. Bank of Nova Scotia*,
691 F.2d 1384 (11th Cir. 1982) ..... 20, 33

*United States v. Barr*,
605 F. Supp. 114 (S.D.N.Y. 1985) ..... 27

*United States v. Cano-Flores*,
796 F.3d 83 (D.C. Cir. 2015) ..... 30

*United States v. Londono-Cardono*,
Crim. No. 05-10304-GAO, 2008 WL 313473 (D. Mass. Feb. 1, 2008) .... 29, 30

*United States v. Miller*,
425 U.S. 435 (1976) ..... 15

*United States v. Peterson*,
812 F.2d 486 (9th Cir. 1987) ..... 29, 30

United States v. Verdugo-Urquidez,
494 U.S. 259 (1990) ..... 25

*United States v. Warshak*,
631 F.3d 266 (6th Cir. 2010) ..... 28

*Walter v. United States*,
447 U.S. 651 (1980) ..... 27

*Zurcher v. Stanford Daily*,
436 U.S. 547 (1978) ..... 24

**Statutes**

15 U.S.C. § 78dd(a) ..... 10

15 U.S.C. § 78j(b) ..... 10

18 U.S.C. § 1962 ..... 10

18 U.S.C. § 1964(c) ..... 11

18 U.S.C. § 2510(15) ..... 18

18 U.S.C. § 2516 ..... 26

18 U.S.C. § 2518 ..... 26

18 U.S.C. § 2701 ..... 11

18 U.S.C. § 2703 ..... passim

18 U.S.C. § 2711(2) ..... 18

18 U.S.C. § 2711(3)(A) ..... 18, 24

Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508
100 Stat 1848 (1986) ..... 3

**Rules**

Fed. R. Crim. P. 41 ..... passim

**Other Authorities**

132 Cong. Rec. S14441-04 (daily ed. Oct. 1, 1986) ..... 32

9A CHARLES ALAN WRIGHT & ARTHUR R. MILLER, FEDERAL PRACTICE AND PROCEDURE
§ 2456 (3d. ed. 2008) ..... 25

Orin S. Kerr, A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It,
72 Geo. Wash. L. Rev. 1208 (2004) ..... 5

**PRELIMINARY STATEMENT**

Google Inc. ("Google") objects to Magistrate Judge Hammer's determination that a warrant (the "Warrant"), issued on probable cause pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) of the Stored Communications Act (the "SCA"), requires it to disclose information in its possession, custody, or control even if such information happens to reside on Google's foreign servers. *See* Google Inc.'s Objections to Magistrate Order ("Google Mem."). Google, a United States company that provides email and cloud computing services, over which this court has jurisdiction, has refused to produce any responsive information unless, when Google looks for it, the information resides on servers located within the United States.

Google excuses its willful non-compliance by pointing to a single case, *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.*, 829 F.3d 197 (2d Cir. 2016) ("*Microsoft*"), *reh'g denied*, 855 F.3d 53 (2d Cir. Jan. 24, 2017) ("*Microsoft II*"). It maintains that, even though Google possesses and controls data responsive to the Warrant from within the United States, and notwithstanding that the Warrant relates to domestic subscribers and fraudulent activity occurring within the United States, *Microsoft* places any data stored on Google servers located outside of the United States beyond the Warrant's reach.

Google is wrong. Judge Hammer correctly ruled that Google's compliance with the Warrant is a purely domestic act, regardless of where the requested data may be stored. Moreover, every court other than the *Microsoft* panel has ruled the same way. As of this date, eleven decisions, issued out of seven different districts, all have held that a warrant issued pursuant to the SCA (1) can require a provider to produce responsive data, even if that provider stores such data on a foreign server; and (2) that such compulsion is not an

impermissible extraterritorial application of the SCA's warrant provisions.[1] Even four Second Circuit judges, all of whom dissented from the Second Circuit's evenly split denial of the government's petition for a rehearing, have exposed the flaws of the *Microsoft* panel's analysis.[2]

In short, not only is *Microsoft* not binding in this District, it was wrongly decided. First, as Judge Hammer noted, *Microsoft* misapplied the analysis the Supreme Court uses to determine whether, if at all, a statute has extraterritorial reach. When properly applied, the disclosure compelled by the Warrant plainly is a permissible territorial application of the SCA. Moreover, the Second Circuit mistook the SCA's grant of power *in rem* as opposed to *in*

---

[1] *In re Search Warrant to Google, Inc.*, No. 16-4116-MAH, 2017 WL 2985391 (D.N.J. July 10, 2017) ("DNJ Decision"); *In the Matter of the Search of Information Associated with [redacted]@gmail.com That Is Stored At Premises Controlled By Google, Inc.,* No. 16-mj-757 (GMH), 2017 WL 2480752 (D.D.C. June 2, 2017) ("DDC Decision I"), motion for order to compel granted, No. 16-mj-757 (BAH), 2017 WL 3445634 (D.D.C. July 31, 2017) ("DDC Decision II"); *In re Search of Information Associated with Accounts Identified as [redacted]@gmail.com and Others Identified in Attachment A That are Stored at Premises Controlled by Google Inc., 1600 Amphitheater Parkway, Mountain View,* CA 94025, No. 2:16-MJ-02197-DUTY-1, 2017 WL 3263351 (C.D. Cal. July 13, 2017) ("CDCA Decision"); *In re: Two Email Accounts Stored at Google Inc.,* No. 17-MJ-1235, 2017 WL 706307 (E.D. Wisc. Feb. 21, 2017) ("EDWI Decision I"), motion to amend warrant denied, No. 17-MJ-1235, 2017 WL 2838156 (E.D. Wisc. June 30, 2017) ("EDWI Decision II"); *In the Matter of the Search of Content That is Stored at Premises Controlled by Google,* No. 16-mc-80263-LB, 2017 WL 1487625 (N.D. Cal. Apr. 25, 2017) ("NDCA Decision"), motion for *de novo* determination denied, No. 16-mc-80263-LB, 2017 WL 3478809 (N.D. Cal. Aug. 14, 2017) ("NDCA Decision II") ; *In the Matter of the Search of Premises Located at [redacted]@yahoo.com, Stored at Premises Owned, Maintained, Controlled, and Operated by Yahoo, Inc.,* No. 6:17-mj-1238, at 3-4 (M.D. Fla. Apr. 7, 2017) ("MDFL Decision"); *In re Search Warrant No. 16-960-M-01 to Google,* 232 F. Supp. 3d 708 (E.D. Pa. Feb. 3, 2017) ("EDPA Decision"), magistrate judge's decision affirmed, No. 16-960-M-1, 2017 WL -- (E.D. Pa. Aug. 17, 2017) ("EDPA Decision II").

[2] *See generally*, *Microsoft II*, 2017 WL 362765 (dissenting opinions of Judges Dennis Jacobs, José A. Cabranes, Reena Raggi, and Christopher F. Droney).

*personam*. That led it to read a territorial limitation into the SCA that does not apply to a court's *in personam* power. Finally, the Second Circuit failed to consider the international consensus that a sovereign nation has the authority to compel someone located within its territory to disclose information within its custody or control, regardless of where the information may be located.

## BACKGROUND

### I. The Stored Communications Act.

Congress enacted the SCA in 1986, as part of the Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986). The government's ability to compel the disclosure of records under the SCA is contained in the section entitled "Required disclosure of customer communications or records." 18 U.S.C. § 2703. It empowers the government to "require the disclosure" of records by electronic communications service and remote computing service providers, such as Google. 18 U.S.C. § 2703(a)-(c). Under the statute's comprehensive framework, certain compelled disclosures require a more demanding showing by law enforcement than others. The nature of that showing is determined by which instrument—subpoena, order, or warrant—is required to compel disclosure of the records in question.

At the low end of the spectrum is the subpoena, which the Government can use to "require the disclosure" by a service provider of the following categories of information:

1. basic subscriber and transactional information concerning a user, 18 U.S.C. § 2703(c)(2);
2. contents of communications in electronic storage with a provider for more than 180 days, 18 U.S.C. § 2703(a) and (b)(1)(B)(i); and
3. other contents of communications stored by a remote computing service, 18 U.S.C. § 2703(b)(1)(B)(i).

These materials may be obtained through any "administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena." 18 U.S.C. §§ 2703(b)(1)(B)(i), (c)(2). The SCA does not require any prior judicial review, based on either probable cause or reasonable suspicion, before the issuance of such subpoenas.

At the intermediate level is a court order pursuant to Title 18, United States Code, Section 2703(d) ("2703(d) order"), which compels a service provider to disclose the following:

1. all records subject to production under a subpoena; and
2. any other "record or other information" concerning a user other than "the contents of communications," such as historical logs of the email addresses in contact with the user, 18 U.S.C. § 2703(c)(1).

A 2703(d) order may be issued where the government provides a court with "specific and articulable facts showing that there are reasonable grounds to believe" that the records sought "are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

Finally, at the high end of the spectrum is an SCA warrant that authorizes government officials to "require the disclosure" by a service provider of the following records:

1. all records subject to production under a 2703(d) order (and therefore also a subpoena); and
2. contents of communications in electronic storage with a provider for fewer than 181 days, 18 U.S.C. § 2703(a).

An SCA warrant may be "issued using the procedures described in the Federal Rules of Criminal Procedure" which require a judicial finding of probable cause based on a sworn affidavit. 18 U.S.C. § 2703(a), (b); *see* Fed. R. Crim. P. 41(d)(1) (requiring probable cause for warrants).

Under this framework, every category of information that the provider must disclose pursuant to a subpoena must also be disclosed pursuant to a 2703(d) order (plus additional categories); and every category of information that the provider must disclose pursuant to a 2703(d) order must, in turn, be disclosed pursuant to a warrant (plus additional categories). *See* 18 U.S.C. § 2703(b)(1)(A), (c)(1)(A) (including a warrant among the instruments that can require the disclosure of records also available pursuant to a court order or subpoena). "The rules for compelled disclosure operate like an upside-down pyramid. . . . The higher up the pyramid you go, the more information the government can obtain." Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1222 (2004). Notably, the language in the statute "requir[ing] . . . disclosure" by the provider remains the same regardless of the instrument employed.

## II. Judge Hammer's Decision.

Judge Hammer issued the Warrant on December 19, 2016. It required Google to disclose the contents of multiple Google email accounts, after finding that the "application for the warrant established probable cause that targets in the United States were engaged in federal criminal activity in the United States, involving United States victims." *DNJ Decision*, 2017 WL 2985391, at *1.

Google produced only certain information it confirmed was stored on its servers in the United States. Relying on *Microsoft*,[3] it refused to disclose other information responsive to the Warrant, including the content of emails and attachments that it stored on its foreign servers. *Id.*

[3] The *Microsoft* and *Microsoft II* decisions are described in detail in Judge Hammer's opinion. *See DNJ Decision*, 2017 WL 2985391, at *5-7.

On April 21, 2017, the Government moved to compel Google to disclose all of the information responsive to the Warrant in its possession, custody, or control, regardless of where Google stored such information. *Id.* Following briefing by the parties and oral argument, Judge Hammer concluded that the "warrant at issue does not violate the presumption against extraterritorial application of United States law" and granted the Government's motion to compel and denied Google's cross-motion to quash. *Id.*

Judge Hammer made a number of factual findings (*id.* at *2, 11 n.8), none of which are disputed:

1. Google stores its data in "shards" that represent a component of a particular email or file. *Id.* at *2. "Individually, these shards are unintelligible; it is not until Google reassembles the relevant shards that they form an intelligible and useable piece of information, such as an e-mail or an attachment to an e-mail." *Id.*
2. Google automatically moves data from server to server, across its network, "and therefore from country to country, as often as once per day." *Id.* Because these components "may move from server to server, and therefore country to country, daily," that the location of such data may "change between the time the warrant is sought from the Court and when it is served on Google." *Id.* (citations omitted).
3. "Google does not consult with the subscriber or account holder regarding where the data will be located . . . . The subscriber or account holder has no role in designating where his or her e-mail content and related data will be stored, and no reasonable expectation that Google will store it in any particular location, or

that the data will remain in that location for a particular period of time." *Id.*

4. When data is copied by Google for purposes of responding to an SCA warrant, the account holder is "not deprived of the use of that data[.]" *Id.* at *11.

5. None of Google's efforts to locate, retrieve, compile, and produce information responsive to an SCA warrant "require any person to actually enter [a] foreign jurisdiction." *Id.* at *11 n.8.

Judge Hammer addressed the "central legal issue in the Government's motion to compel, [and the decision] in *Microsoft*." Whether requiring a provider to produce information in its possession, custody, or control, and regardless of the location of the information, violates the canon of statutory construction known as the presumption against extraterritoriality. *Id.* at *3-4. To resolve that, he applied the two-step framework set forth in *Morrison v. National Australia Bank Ltd.*, 561 U.S. 247 (2010).

At the first step, he concluded that there was no clear expression by Congress that the SCA's warrant provisions were intended to be extraterritorial. *Id.* at *4, 8-9 (to determine whether a particular application is domestic or extraterritorial, a "court must identify the focus of the statute, and then determine whether the conduct relevant to that focus occurs or would occur in the United States.") (citing *RJR Nabisco, Inc. v. European Community*, 136 S. Ct. 2090, 2101 (2016). At the second step, he concluded that "compelling Google to provide all responsive information to the search warrant issued in this matter, regardless of whether the information is stored on computer servers outside of the United States, does not violate the presumption against extraterritorial application of United States law because the conduct relevant to

the extraterritorial[ity] analysis—*i.e.*, the location of the search—occurs entirely in the United States." *Id.* at *9.

## ARGUMENT

### I. Requiring Google To Produce Information In Its Possession, Custody, Or Control Is A Domestic Application Of The SCA's Warrant Provisions.

The "central issue" before Judge Hammer was whether a search warrant issued pursuant to the SCA, "which requires an e-mail service provider to produce data that is responsive to the search warrant but stored on computer servers outside the United States, violates the presumption against extraterritorial application of United States law." *DNJ Decision*, 2017 WL 2985391, *3. In *Morrison v. Nat'l Australia Bank, Ltd.*, 561 U.S. 247 (2010), and *Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659 (2013), the Supreme Court "provided a [two-step] framework to determine whether a particular statute applies extraterritorially." *DNJ Decision*, 2017 WL 2985391, at *3-4. "At the first step, [a court must] ask whether the presumption against extraterritoriality has been rebutted – that is whether the statute gives a clear, affirmative indication that it applies extraterritorially."[4] *RJR Nabisco,* 136 S. Ct. at 2101. At the second step, triggered only if a provision is found not to apply extraterritorially, courts must determine whether the case nonetheless "involves a domestic application of the statute . . . by looking to the statute's 'focus.'" *Id.* Ultimately, if the relevant conduct "occurred in the United States,

[4] Judge Hammer's opinion suggests that the Government argued, under step one of the *Morrison* analysis, that the SCA's warrant provisions were intended by Congress to be an extraterritorial piece of legislation. *DNJ Decision*, 2017 WL 2985391, at *8-9. In fact, "the government does not argue that, for purposes of step one of the *Morrison* analysis, the SCA was intended to be extraterritorial." It argued instead that "[w]hat matters here is whether the instant case involves a domestic ***application*** of the SCA's warrant provisions" under step two of the *Morrison* analysis. Reply Memorandum of Law in Further Support of the Government's Motion for an Order Directing Google to Comply with a Warrant for Disclosure of Records ("Gov't Reply") at 19 (emphasis in original).

then the case involves a permissible domestic application ***even if other conduct occurred abroad***." *Id.* (emphasis added).

### A. The "Focus" Of The SCA's Warrant Provisions Is Required "Disclosure."

That the focus of Section 2703 is on disclosure is apparent not only from its title—"Required disclosure of customer communications or records"— but also from that in each subsection, the same requirement (*i.e.*, to disclose) applies without regard to the type of process that must issue as a precondition to the requirement. *See* 18 U.S.C. § 2703(b) (creating the same authority to require disclosure pursuant to warrants, subpoenas, and court orders under Section 2703(d)); *see also* § 2703(c) (requiring disclosure pursuant to warrants, subpoenas, court orders, consent, and certain written requests). Once the statute's requirements are met, the end result is that the provider is compelled to disclose the information described. It is difficult to conceive of a section whose focus on disclosure could be clearer.

Nonetheless, the *Microsoft* court concluded that Section 2703's warrant provision evokes a focus on privacy because "Rule 41 is undergirded by the Constitution's protections of citizens' privacy[.]" 829 F.3d at 217 (quotations omitted). It then looked to other sections of the SCA, noting that various provisions included mechanisms designed to protect individuals' "privacy interest in their stored communications." *Id.* at 217-18. That was error. A proper extraterritoriality analysis is conducted on a section by section basis. *See, e.g.*, *Morrison*, 561 U.S. at 263–65 (holding that Section 10(b) of the Securities Exchange Act of 1934, 15 U.S.C. § 78j(b), does not apply extraterritorially, but that Section 30(a), 15 U.S.C. § 78dd(a), does); *RJR Nabisco*, 136 S. Ct. at 2100-11 (holding that RICO's substantive provisions, 18 U.S.C. § 1962, apply extraterritorially to the extent the charged predicates

apply extraterritorially, but that RICO's civil damages provision, 18 U.S.C. § 1964(c), does not).

Google is simply wrong when it argues this Court must "take into account the whole statute and related legislation." Google Mem. at 18 n.4. To do so tramples the distinction Congress drew between the act of access—the focus of Section 2701—and the act of disclosure—the focus of Section 2703. Judge Cabranes made this point through a compelling textual analysis in his dissent from the denial of rehearing in *Microsoft*. He explained that because Congress clearly identified those situations where "access" was the focus of a section – as with Section 2701's unlawful access provisions – it must have signaled a different focus in Section 2703, which repeatedly emphasizes ***disclosure*** as opposed to ***access***. *Microsoft II*, 855 F.3d at 67-68 (Cabranes, J., dissenting); *see also DDC Decision II*, 2017 WL 3445634, at *24 ("The *Microsoft* panel erred by assuming that if the focus of the statute was 'privacy,' then the provider's 'access' to the user's electronic information was the conduct relevant to the focus of the statute. As Judge Cabranes explained in dissent, this assumption is belied by the language and structure of the SCA.").

It is only by arguing in broad policy terms that Google can credibly maintain that SCA has but one focus: Privacy. It is improper to analyze statutes at such a general level, as *Morrison* makes clear. 561 U.S. at 263-65. Notwithstanding the broader "public interest" goal of protecting U.S. investors and the integrity of U.S. markets, when determining the territorial reach of the Exchange Act, the Court focused on the actual mechanism enacted by Congress for addressing its larger policy goals as determined by the statutory text. For the Exchange Act, that mechanism was the regulation of certain types of securities transactions. For the SCA, that mechanism is the regulation of compelled disclosure. Such disclosure occurs domestically in response to

an SCA warrant and is, therefore, a domestic application of the statute's warrant provisions.

**B. Even Under Google's Privacy-Centric Reading Of Section 2703, The SCA Operates Domestically.**

In *RJR Nabisco*, the Supreme Court held that where "conduct relevant to the statute's focus occurred in the United States, then the case involves a permissible domestic application ***even if other conduct occurred abroad***." *RJR Nabisco*, 136 S. Ct. at 2101(emphasis added). Accordingly, Judge Hammer properly addressed the "conduct relevant to the focus" of the SCA and held, even assuming that Section 2703's focus is privacy[5], any invasion of the customer's privacy occurs when the information is disclosed to the government in the United States and searched, pursuant to the warrant by investigators, in the United States.

The Warrant does not require Google to search for evidence of the specified federal offenses. *Compare* Warrant Attachment B.I (describing the materials Google is required to disclose), *with* Warrant Attachment B.II (describing the information the government may search for and seize). Rather, the search of the disclosed information is conducted, by the government, in the United States. This two-step approach—first the disclosure of information by a provider, and second, its search by law enforcement—reflects that Google is simply a custodian of certain information the court has determined should ultimately be searched by law enforcement for evidence of crime.[6]

---

[5] He noted, however, the "strong support" for the Government's position that the focus of Section 2703 is disclosure, not privacy, and that any privacy interest are protected by the way disclosure are regulated. *DNJ Decision*, 2017 WL 2985391 at *9 n. 6.

[6] See I*n the Matter of the Search of Information Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.,* 13 F. Supp. 3d 157 (D.D.C. 2014) (approving of the two-step approach to email

Under *Morrison*, conduct relevant to the focus of a statute is narrower than simply ***any*** conduct leading up to or related to conduct regulated by the statute; it is the conduct (here, disclosure) that the statute regulates. *See also DDC Decision II*, 2017 WL 3445634, at *24 (holding that "[r]egardless of whether the focus of § 2703 is 'privacy,' 'disclosure,' or both, however, the conduct relevant to that 'focus' is the same: disclosure" and does not include Google's "preparatory acts necessary" for responding to an SCA warrant). Google's formulation—that Section 2703 includes ***all*** of its conduct leading up to the disclosure responsive to an SCA warrant—stretches the holding in *Morrison* beyond recognition. As noted by the Chief Judge for the District of D.C.:

> Google's reading of *RJR Nabisco* would inexorably lead to an impractical rule impossible to apply. For example, … in a prosecution for distribution of narcotics in the United States, the "cultivation, processing, manufacturing, packaging, shipping, payment for the supply, managing and supervision of the distribution" may all have occurred abroad, but such preparatory acts to the criminal conduct of illegal narcotics distribution in the United States do not render the prosecution of drug offenses in the United States an extraterritorial application of the applicable statutes.

---

search warrants because "[e]nlisting a service provider to execute the search warrant could also present nettlesome problems"); *In the Matter of a Warrant for All Content & Other Info. Associated with the E-mail Account xxxxxxx gmail.com Maintained at Premises Controlled By Google, Inc.*, 33 F. Supp. 3d 386, 395 (S.D.N.Y. 2014), as amended (Aug. 7, 2014) (approving of two-step process in part because "[p]lacing the responsibility for performing these searches on the email host would also put the host's employees in the position of appearing to act as agents of the Government vis-à-vis their customers").

*DDC Decision II*, 2017 WL 3445634, at *25. Rather, the relevant provisions of Section 2703 are focused on a requirement to disclose, placed upon a provider, within a court's jurisdictional reach, that occurs in the United States.

Google is simply wrong when it argues that any conduct it takes in response to an SCA warrant must be considered in analyzing the scope of Section 2703. Moreover, it fails to identify any conduct that it actually is required to undertake outside of the United States. Google argues that for purposes of conducting an extraterritoriality analysis, this court must not only consider where the disclosure occurs, but also the provider's conduct in "querying its network to identify responsive communications located in data centers outside the United States, accessing those foreign-stored communications, and retrieving them to the United States for disclosure to the government …." Google Mem. at 16. Google labors to characterize such conduct as conduct that occurs outside of the United States, but as Judge Hammer noted, "[r]equiring Google to query its servers for responsive data does not require any person to actually enter the foreign jurisdiction." *See DNJ Decision*, 2017 WL 2985391, at *11 n.8; *see also DDC Decision II*, 2017 WL 3445634, at *25 (recognizing that "all of the preparatory conduct that Google strains to place abroad, actually happens in the United States and constitutes a domestic application of the statute"). While data may flow from Google's foreign servers to the U.S. in the process, it does so in response to keystrokes made in Mountain View, California.[7]

[7] Google nevertheless argues that although its conduct occurs domestically, the fact that "Google has technology that permits it to easily control data located in faraway places with ease does not mean that nothing happens in those faraway places." Google Mem. at 22. But the question is not whether anything that happens overseas; rather, it is whether relevant conduct occurs overseas and Google points to none. *RJR Nabisco*, 136 S. Ct. at 2101 (conduct abroad is not relevant if the statute focuses on conduct occurring

Simply put, the role of the provider in disclosing the information to be searched pursuant to the SCA is precisely like the role of any party compelled to produce information. Contrary to Google's assertion that an SCA warrant requires Google to "seize" information it already possesses, Google Mem. at 13, persons compelled to produce documents are not deemed to be agents of the government simply because they comply with their obligations ordered by a court or subpoena. *See, e.g.*, *United States v. Miller*, 425 U.S. 435, 443-44 (1976) (finding that bank responding to subpoena for bank records is not an agent for the government, and applying the "general rule that the issuance of a subpoena to a third party to obtain the records of that party does not violate the rights of a defendant, even if a criminal prosecution is contemplated at the time . . . the subpoena is issued"); *Microsoft II*, 855 F.3d at 73 ("we need to convene *en banc* to clarify that a service provider who complies with a § 2703(a) warrant … does not thereby conduct a search or seizure as the agent of the government") (Raggi, J., dissenting). Google is neither required to seize control over information in someone else's possession nor to review it for evidence of an offense. It is required to produce information that is already in its possession and custody, which it controls from the United Sates, regardless of where it may be stored. Moreover, any search of content pursuant to information obtained through the SCA occurs only after the disclosure has been made by a provider in the United States.

Indeed, although Google's brief uses terms like "seizure" to describe its collection of information it controls in response to an SCA warrant, it has

---

domestically). The fact that law enforcement could not, using a traditional Rule 41 search warrant, search and seize foreign servers is also of no import. Here, the relevant question is whether the provider, which can retrieve such data "easily," can be compelled to disclose it. *Id.*

conceded in related litigation that it does not act as an agent of the Government when responding to an SCA warrant. It, therefore, critically departs from the *Microsoft* holding as recently described by a magistrate judge in the District of D.C.:

> In *Microsoft*, the finding that the service provider was "acting as an agent of the government" when searching data centers in Ireland was critical to the court's conclusion that a service provider is "seizing" a customer's data and invading that customer's privacy at the data's storage site. *Microsoft*, 829 F. 3d at 220. Google's concession that it acts through its own agency when complying with an SCA warrant thus undermines the Second Circuit's holding in *Microsoft*. But its concession is also well taken. A service provider is not properly viewed as acting as an agent of the government when "seizing"—or, more appropriately, simply accessing—customer content pursuant to an SCA warrant. *See Microsoft II*, 855 F.3d at 72–73 (Raggi, J., dissenting).

*DDC Decision I*, 2017 WL 2480752 (citations omitted).

## II. The SCA Provides Courts With Power *In Personam* To Require U.S. Providers To Produce Information In Their Custody Or Control, Regardless Of The Location Of The Information.

Google argues that "Congress used the term of art 'warrant' to invoke the traditional limitations associated with that term" and that "a warrant protects privacy in a distinctly territorial way." *See* Google Mem. at 12-14 (citing *Microsoft*, 829 F.3d at 212). According to Google, Congress's use of the term "warrant" somehow "made clear that SCA warrants . . . are territorially limited."[8] Google Mem. at 12.

[8] Judge Hammer's decision indicates that "to the extent the Government relies on *in personam* jurisdiction to satisfy the first step of *Morrison*, the argument fails …." *DNJ Decision*, 2017 WL 2985391, at *8. However, "the government does not argue that, for the purposes of step one of the *Morrison* analysis, [that] the SCA was intended to be extraterritorial." Gov't Reply at 19.

Google is wrong. The SCA grants courts *in personam* power—*i.e.*, power over a person as opposed to *in rem* power over property—to require certain providers, including email providers, to produce certain information responsive to a warrant. Accordingly, and as detailed below, an SCA warrant is critically different from a traditional Rule 41 search warrant, such that the territorial limitations historically associated with traditional search warrants do not apply in this context.

### A. The SCA Grants Courts Power *In Personam* To Compel Providers To Produce Information.

Unlike searches for physical items, or even electronically stored information on a defendant's computer or cellular phone, the data at issue here, primarily email content or other files stored in the "cloud," is truly intangible. The concept of an "original" email is inapposite. Accordingly, the Warrant, like all SCA warrants, requires only the production of copies[9] of responsive data. An SCA warrant seeks the data itself, untethered from any physical or tangible item. *See Microsoft II,* 855 F.3d at 61 ("Electronic 'documents' are literally intangible: when we say they are stored on a disk, we mean they are encoded on it as a pattern.") (Jacobs, J., dissenting). Therefore, while Rule 41, generally designed to deal with tangible items, *see generally* Rule 41, is ill-equipped to deal with the type of information sought by an SCA warrant, the SCA, on the other hand, is specifically tailored to the unique nature of data at issue by focusing on courts' *in personam* authority over providers that control such data. *See, e.g.*, *EDWI II Decision*, 2017 WL 2838156, at *4 ("Unlike a traditional search warrant, which commands law

[9] Even the term "copy" is loaded in that it suggests that there is an "original." When dealing with emails produced from an email provider, these distinctions are meaningless.

enforcement to do certain things, *see* Fed. R. Crim. P. 41(e)(2)(A), a warrant under 2703 compels action by a service provider."); *NDCA Decision*, 2017 WL 1487625, at *4 ("[A]n SCA warrant is not a search warrant in the classic sense, the government does not search a location ….").

The *in personam* nature of the SCA's grant of power is clear from the threshold jurisdictional question raised by an application for a warrant under the SCA: whether the requested warrant is directed at an entity that the SCA covers, namely, providers of electronic communication services or remote computing services. *See* 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) (all sections of the SCA allowing the government to compel production of records under a warrant, but only with respect to "electronic communication service" or "remote computing service" providers); *see also* 2510(15) (defining "electronic communication service" providers); 2711(2) (defining "remote communication service" providers).

Moreover, since its amendments in 2001, the SCA explicitly broadened the jurisdiction of courts to issue warrants for information located outside of the district, marking a departure from Rule 41(b)(1)'s more traditional *in rem* jurisdictional requirement, which is typically focused on the territorial reach of a magistrate judge's authority. In addition to conferring jurisdiction when the information is stored in the same district, the SCA now defines a "court of competent jurisdiction" as a court having jurisdiction over the offense under investigation or a court in the district in which the provider is located. *See* 18 U.S.C. § 2711(3)(A) (defining a "court of competent jurisdiction" to include any "district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that … has jurisdiction over the offense being investigated"). Accordingly, under the broader jurisdiction granted by the SCA, the information required to be disclosed pursuant to a

warrant need not be in this district at the time the warrant is issued.

### B. The SCA Allows Courts To Compel U.S. Providers To Produce Information Within Their Custody Or Control Irrespective Of Where The Data Is Located.

That the SCA grants courts *in personam* power over providers is significant given the long line of cases holding that a court's power over a person properly before it permits the court to require that person to take certain acts either within, or outside of, its territorial jurisdiction. *See, e.g.*, *State of New Jersey v. City of New York,* 283 U.S. 473, 482 (1931) ("Defendant contends that, as it dumps the garbage into the ocean and not within the waters of the United States or of New Jersey, this Court is without jurisdiction . . . [b]ut the defendant is before the Court and . . . [t]he situs of the acts . . . whether within or without the United States, is of no importance. Plaintiff seeks a decree *in personam* ...."); *Steele v. Bulova Watch Co., Inc.*, 73 S. Ct. 252, 257 n.17 (1952) ("the District Court in exercising its equity powers may command persons properly before it to cease or perform acts outside its territorial jurisdiction"); *Republic of the Philippines v. Marcos*, 862 F.2d 1355, 1363-64 (9th Cir. 1988) ("The injunction is directed against individuals, not against property . . . Because the injunction operates *in personam*, not *in rem*, there is no reason to be concerned about its territorial reach").

This fundamental principle has consistently been applied in the specific context addressed by Section 2703—the compelled disclosure of information. If a person or entity with custody or control over such information is properly before a court with *in personam* jurisdiction over that person, an order to produce applies to all information over which that custody or control can be exercised, regardless of whether the information is stored within the district, elsewhere in the United States, or abroad. *See, e.g.*, *Hay Group, Inc. v. E.B.S.*

*Acquisition Corp.*, 360 F.3d 404, 412 (3d Cir. 2004) (Alito, J.) ("'Production' refers to the delivery of documents, not their retrieval, and therefore 'the district in which the production . . . is to be made' is not the district in which the documents are housed but the district in which the subpoenaed party is required to turn them over."); *Gerling Int'l Ins. Co. v. CIR,* 839 F.2d 131, 140 (3d Cir. 1988) (explaining that, under the rule governing the production of documents and other evidence in tax court, "[t]he location of the documents, whether within the territorial jurisdiction of the court or not, is irrelevant"); *United States v. Bank of Nova Scotia*, 691 F.2d 1384, 1389-90 (11th Cir. 1982) (affirming the district court's order enforcing a grand jury subpoena against a Bahamian bank which was "subpoenaed while subject to the jurisdiction of [the district court]," where the subpoena required disclosure of records located in the Bahamas); *Marc Rich & Co. v. United States*, 707 F.2d 663, 667 (2d Cir. 1983) (a witness may not "resist the production of [subpoenaed] documents on the ground that the documents are located abroad … [t]he test for production of documents is control, not location") (citations omitted); *see also* 9A CHARLES ALAN WRIGHT AND ARTHUR R. MILLER, FEDERAL PRACTICE AND PROCEDURE § 2456 at 31 ("[E]ven records kept beyond the territorial jurisdiction of the district court . . . may be covered if they are controlled by someone subject to the court's jurisdiction.").[10] Because a court's ability to require disclosure is premised on

[10] *See also Reinsurance Co. of Am. v. Administratia Asigurarilor de Stat (Admin. of State Ins.)*, 902 F.2d 1275, 1281 (7th Cir. 1990) ("A court or agency in the United States, when authorized by statute or rule of court, may order a person subject to its jurisdiction to produce documents, objects, or other information relevant to an action or investigation, even if the information … is outside the United States.") (quoting RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW § 442); *In re Anschuetz & Co., GmbH*, 754 F.2d 602, 614 n.29 (5th Cir. 1985) (noting that "[i]t is not *ipso facto* a defense to a discovery request that the law of a foreign country may prohibit production or disclosure. As the Eleventh Circuit held in *United States v. Bank of Nova Scotia*, 691 F.2d 1384

the court's jurisdiction over the person, the compulsion—that is, requiring that person to produce documents—is *not* extraterritorial.

Significantly, and consistent with the Supreme Court's decision in *RJR Nabisco*, this conclusion remains the same even when some of the information required to be disclosed must be gathered from outside the United States. *See* Restatement (Third) of Foreign Relations Law § 442(1)(a) (1987) (making clear that "[a] court or agency in the United States, when authorized by statute or rule of court, may order a person subject to its jurisdiction to produce documents, objects, or other information relevant to an action or investigation, even if the information or the person in possession of the information is outside the United States"). Courts have long been empowered to exert authority on people and entities over whom they have jurisdiction, even if that authority has consequences overseas or otherwise outside of a court's territorial jurisdiction. *See, e.g., Blackmer v. United States*, 284 U.S. 421, 438 (1931) ("The jurisdiction of the United States over its absent citizen, so far as the binding effect of its legislation is concerned, is a jurisdiction *in personam*, as he is personally bound to take notice of the laws that are applicable to him and to obey them."); *Hale v. Henkel*, 201 U.S. 43, 75 (1906) ("It would be a strange anomaly to hold that a state, having chartered a corporation to make use of certain franchises,

---

(11th Cir.1982), even at the sanction stage, violation of foreign law is not necessarily a valid defense to a lawfully issued subpoena for documents."), *cert. granted, judgment vacated on other grounds sub nom. Anschuetz & Co., GmbH. v. Mississippi River Bridge Auth.*, 483 U.S. 1002 (1987); *In re Sealed Case*, 832 F.2d 1268, 1284 (D.C. Cir. 1987), *abrogated on other grounds by Braswell v. United States*, 487 U.S. 99 (1988) (holding that a subpoena for documents in Switzerland is enforceable by the District Court if it has personal jurisdiction over the companies whose records are sought); *Sec. & Exch. Comm'n v. Minas De Artemisa, S. A.*, 150 F.2d 215, 218 (9th Cir. 1945) ("The obligation to respond applies even though the person served [with a subpoena] may find it necessary to go to some other place within or without the United States in order to obtain the documents required to be produced.").

could not, in the exercise of its sovereignty, inquire how these franchises had been employed, and whether they had been abused, and demand the production of the corporate books and papers for that purpose.").

This fundamental concept—that a court's power to compel disclosure is directed to the person (*in personam*), not the items to be produced (*in rem*)—was well-established at common law long before Congress enacted Section 2703 of the SCA in 1986. "'[W]hen a statute covers an issue previously governed by the common law,' [courts] must presume that 'Congress intended to retain the substance of the common law.'" *Kirtsaeng v. John Wiley & Sons, Inc.*, 133 S. Ct. 1351, 1363 (2013) (quoting *Samantar v. Yousuf*, 560 U.S. 305, 320 n.13 (2010)). In light of the settled common law on the *in personam* nature of a court's power to compel the disclosure of documents, as well as Section 2703's focus on regulating such disclosure, there should be no doubt that Congress envisioned "a court of competent jurisdiction" as one empowered to compel a U.S.-based provider of electronic communications service or remote computer service to disclose information in its custody and control—regardless of where that information may be when the provider takes action in the United States to gather it. *See EDWI Decision I*, 2017 WL 706307, at *3 ("Provided the service provider is within the reach of the court, the court may lawfully order that service provider to disclose data in the service provider's custody and control, without regard of where the service provider might choose to store the ones and zeros that comprise the relevant data.").

### C. Congress's Use Of The Term "Warrant" Was Meant To Import The Probable Cause Standard, Not To Impose A Territorial Limit.

Google argues that "Congress used the term of art 'warrant' to invoke the traditional limitations associated with that term" and that "a warrant protects privacy in a distinctly territorial way." *See* Google Mem. at 12-14 (citing

*Microsoft*, 829 F.3d at 212). That is wrong.

Congress, in enacting the SCA, could have—but did not—simply require the government to obtain a Rule 41 warrant to obtain communications held by a provider. Instead, it created a statutory requirement to disclose that was activated by the issuance of a new kind of warrant, one that operates much differently than a traditional warrant. A traditional warrant authorizes a law enforcement officer to take certain investigatory actions within a particular jurisdiction. That is not how an SCA warrant operates. If it did, such a warrant would only allow law enforcement agents to enter Google's premises and conduct searches for relevant records there. Instead, the text of the SCA plainly states that providers are compelled to disclose records to the government. *See* 18 U.S.C. § 2703 (various subsections allowing a governmental entity to "require" a provider to "disclose" the contents of communications or other records). That Congress required the government to use the "***procedures***" in the Federal Rules of Criminal Procedure for obtaining the warrant, shows that Congress knew that it was creating a new technique for compelling the disclosure of records and that it wanted it governed by existing procedures for traditional warrants. 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A) (emphasis added).

Google argues that Congress must have been referring to a territorial requirement, because Congress would have otherwise referred to an SCA warrant as an order issued upon a showing of probable cause. Google Mem. at 11-12. Not so. That Congress sought to piggyback on the ***procedures*** set forth in Rule 41 does not in any way suggest that it sought to impose territorial restrictions on SCA warrants, beyond those that relate to *in personam* jurisdiction over U.S. providers. In fact, the portion of Rule 41 that imposes such limitations is supplanted by the SCA's directive that a court could issue

an SCA warrant regardless of whether the provider or the data sits within its geographical jurisdiction. *Compare* 18 U.S.C. §§ 2703(a)-(c) (requiring in certain circumstances a "warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction") and 2711(3)(A)(i) (defining a "court of competent jurisdiction" to include any court of the United States that "has jurisdiction over the offense being investigated"), *with* Rule 41(b)(1) (authorizing a magistrate judge to "issue a warrant to search for and seize a person or property located within the district").[11]

Google also argues that "[s]earch warrants are not directed at persons; they authorize the search of 'places' and the seizure of 'things.'" Google Mem. at 14 (citing *Zurcher v. Stanford Daily*, 436 U.S. 547, 555 (1978)). Rather than address what the SCA does—conferring power to courts to compel providers to produce information—Google bases its claim on the following syllogism: an SCA warrant is a warrant, and the *Zurcher* court held that warrants apply to places and things, not people; therefore an SCA warrant should be treated as though it applies to places and things, not people (or providers). Yet *Zurcher* clearly involved a traditional Rule 41 search warrant and, indeed, was decided eight years before Congress enacted the SCA, which is, by its own terms, directed at persons (*i.e.*, providers).

Google then relies on *United States v. Verdugo-Urquidez* for the proposition that a traditional warrant would be a "dead letter outside the United States" in an attempt to characterize the warrant requirement as one

[11] Although Judge Hammer indicated that "[t]he Government's *in personam* jurisdiction argument is difficult to reconcile with the territorial limitations in Rule 41(b)," those very restrictions are the ones statutorily supplanted by the SCA. *DNJ Decision*, 2017 WL 2985391, at *8.

that protects privacy in a territorial way. 494 U.S. 259, 274 (1990); *see* Google Mem. at 13. Google ignores, however, that *Verdugo-Urquidez* did not hold that the Fourth Amendment's warrant requirement protects privacy in a territorial way; indeed, the Court ultimately declined to hold that the Fourth Amendment was violated by the warrantless overseas search. *Verdugo-Urquidez*, 494 U.S. at 274. Rather, the Court held that a U.S. warrant would be a "dead letter" in another country because the physical premises searched was outside of a U.S. magistrate's reach, a conclusion that is unsurprising given the territorial restrictions of Rule 41.

In contrast, this case involves an SCA warrant, which empowers courts to compel production from U.S. providers like Google. There is no question that providers like Google are within this Court's reach. Accordingly, Google's reliance on both *Zurcher* and *Verdugo-Urquidez* essentially wishes away the key distinction between an SCA warrant and a traditional search warrant—that an SCA warrant creates authority over providers (*in personam*) and not on places and things (*in rem*).

Moreover, to the extent that the SCA seeks to protect privacy, it does so ***substantively*** through the probable cause requirement, not ***arbitrarily*** based on where a provider decides to store data. *See Microsoft II,* 855 F.3d at 75 ("Congress addressed [privacy] concerns through the warrant requirement in the SCA … [which] provides protection for individual privacy interests by requiring the Government to make an adequate showing of probable cause.") (Droney, J., dissenting); *id.* at *6 ("Important as privacy is, it is in any event protected by the requirement of probable cause; so a statutory focus on privacy gets us no closer to knowing whether the warrant in question is enforceable.") (Jacobs, J., dissenting). Indeed, as the legislative history of the SCA makes clear, the SCA is "designed to protect legitimate law enforcement needs while

minimizing intrusions on the privacy of system users" by providing "***standards*** by which law enforcement agencies may obtain access to both electronic communications and the records of an electronic communication system." 132 Cong. Rec. S14441-04 (1986) (emphasis added).[12] The goal of ensuring that probable cause exists, however, has no significance on whether an SCA warrant operates extraterritorially.

**D. Google's Purported "Caretaker" Status Is Irrelevant.**

Google likened itself below to a caretaker of its users' communications, contending that compelling it to disclose its foreign-stored information is "the equivalent of requiring a hotel chain to search, seize, and retrieve to the United States luggage or correspondence a customer has stored in a room in a foreign hotel." *DNJ Decision*, 2017 WL 2985391, at *11 n.8. Judge Hammer "readily dismissed" that analogy, however, in part because "[r]equiring Google to query

[12] Google points to the Wiretap Act's reference to an order supported by "probable cause" as a basis for finding that the SCA's reference to a "warrant" was not meant only to import the probable cause requirement. Google Mem. at 11-12 (citing 18 U.S.C. § 2518(3)). However, this provision's use of the term "probable cause" was made uniquely necessary by the fact that a finding of probable cause alone is insufficient to obtain the order. *See* 18 U.S.C. § 2518(3)(c) (incorporating an necessity requirement). *See also* 18 U.S.C. §§ 2516 and 2518(1)(a) (both requiring authorization to file an application from a high-ranking law enforcement attorney). Because the requirement to obtain a wiretap order requires *more* than just probable cause, it is no surprise that Congress needed to refer to that standard specifically in order to lay out the government's requisite showing for a wiretap. Moreover, given that Section 2518 deals with the interception of live communications, as opposed to stored communications that already exist and are stored by the provider, Congress's use of the term "warrant" would have been more confusing than helpful. In the context of the SCA, on the other hand, the use of the term "warrant" immediately brings to mind the probable cause standard. Where the appropriate standards for legal processes defined in the SCA are not immediately apparent, as is with the case of court orders under Section 2703(d), Congress was required to articulate the standard within the statutory text.

its servers for responsive data does not require any person to actually enter the foreign jurisdiction." *Id.* Google resurrects that argument, contending "the communications obtained with a warrant are not the provider's business records or information conveyed to the provider by the customer; they are the customer's private communications." Google Mem. at 19-20.

Google's position (1) draws an irrelevant distinction under any Fourth Amendment analysis; (2) is contrary to any reasonable interpretation of Section 2703; and (3) is untrue as a matter of fact. First, if anything, there is no basis for concluding that information held by third-party custodians is entitled to ***greater*** privacy protection than records directly held by an individual. There is even less of a basis here, where Google is arguing that such heightened protection applies only to foreign-stored, as opposed to domestically-stored, information. *See, e.g.*, *Fisher v. United States*, 425 U.S. 391, 401, 408-09 (1976) (holding that the Fourth Amendment's reasonableness requirement applies to a summons or subpoena compelling the production of private papers held by criminal defendants' attorneys); *cf. Hale v. Henkel*, 201 U.S. 43, 73-76 (1906) (the Fourth Amendment imposes a reasonableness requirement in the context of compelled disclosure of a corporation's records); *United States v. Barr*, 605 F. Supp. 114 (S.D.N.Y. 1985) (upholding a subpoena to a bailee to produce mail).[13] There is no rational basis for distinguishing cases relied on by the government involving a court's ability to compel the recipients of a subpoena from producing documents within their possession, custody, or control.

[13] Although a warrant may be required to *search* information lawfully *obtained* by law enforcement without a warrant, *see Walter v. United States*, 447 U.S. 651, 655 (1980), an SCA warrant nevertheless authorizes the search of information obtained from a provider.

Second, Google's "caretaker" argument is inconsistent with the text of Section 2703. Google claims that Congress decided to require a warrant for the "content of communications, which it deemed most private" because "[u]nlike the subscriber information obtained with a subpoena or the customer records obtained with a court order, the communications obtained with a warrant are … the customer's private communications…." Google Mem. at 19-20. That, however, ignores that the SCA does not always require a Warrant in order to obtain a user's content. Instead, Section 2703 specifically authorizes disclosure by subpoena for communications that are over 180 days old and are held by an electronic communications service, or for ***any*** communications held by a remote computing service. *See* 18 U.S.C. §§ 2703(a), (b)(1)(B). Although such disclosures require the government to give prior notice to the subscriber, that notice may be delayed with the court's approval. *See* 18 U.S.C. § 2703(b)(1)(B). That the SCA permits the government to obtain content with a subpoena or court order, as opposed to a warrant, and without prior notice to the subscriber, completely undermines Google's assertion that Congress intended a territorial restriction to apply to the content of communications by using the term "warrant" in the SCA.[14]

Finally, according to Google's own filings in other litigation matters, it acts nothing like a hotel storing its guests' luggage or a bank providing a customer a safe deposit box because unlike those entities, which respect the

[14] This is not to say that the Fourth Amendment might not provide greater protection than the SCA. *See, e.g.*, *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010). However, assuming that obtaining such content via subpoena or court order (as opposed to a warrant) under the SCA runs afoul of the Fourth Amendment, Congress, nevertheless enacted the SCA to allow such content to be obtained without a warrant, which is wholly inconsistent with Google's characterization of Congress's intentions in using the term "warrant" in the SCA.

privacy of the contents they hold, Google regularly reviews its users' content. *See* Google Inc.'s Answer to Plaintiffs' Amended Complaint ¶ 1, No. 15-cv-04062-LHK (N.D. Cal. Oct. 21, 2016), ECF No. 59 ("Google admits that it offers Gmail, a web-based email service, to users, that it does not charge Gmail users money for their use of Gmail, and that it applies automated processing to certain emails to identify information that is used to provide various Google services and product features, including relevant advertising."); Defendant Google Inc.'s Motion to Dismiss Plaintiffs' Consolidated Individual and Class Action Complaint; Memorandum of Points and Authorities in Support Thereof at 11, No. 13-md-02430-LHK, ECF No. 44 ("Here, all Plaintiffs who are Gmail users consented to the automated scanning of their emails (including for purposes of delivering targeted advertising) in exchange for using the Gmail service."). Put simply, electronically scanning its users' emails for its own commercial purposes is a central part of Google's business model and not anything like the way a hotel or bank treats customers.

**E. Google's Analogy To The Wiretap Act Is Unavailing.**

Judge Hammer accepted Google's analogy between the SCA and the Wiretap Act. He held that, although the Wiretap Act gives courts *in personam* power over certain providers, numerous courts have held that the Wiretap Act has no extraterritorial application. Accordingly, he concluded "even if the SCA established *in personam* jurisdiction, that would not necessarily suffuse the SCA with extraterritorial application." *DNJ Decision*, 2017 WL 2985391, at *8 (citing *United States v. Peterson*, 812 F.2d 486 (9th Cir. 1987) and *United States v. Londono-Cardono*, Crim. No. 05-10304-GAO, 2008 WL 313473 (D. Mass. Feb. 1, 2008). However, both *Peterson* and *Londono-Cardono* involve situations where a wiretap was conducted by foreign law enforcement in a foreign

country, and in both instances the courts held that U.S. law enforcement could use the evidence obtained from such wiretaps without meeting the requirements of the Wiretap Act. *See Peterson*, 812 F.2d at 489-92 (addressing the admissibility of evidence derived from a wiretap conducted in the Philippines by Philippines law enforcement); *Londono-Cardono*, 2008 WL 313473, at *1-2 (Colombian wiretap). *Peterson* and *Londono-Cardono* merely stand for the proposition that the Wiretap Act is not extraterritorial, in terms of step one of the *Morrison* analysis, an issue the government does not contest with respect to the SCA. The question before this Court is whether the conduct at issue is an ***extraterritorial application*** of SCA. Google's position here is more akin to a U.S. telecom provider with a facility in Mountain View, California, ordered to assist in facilitating a wiretap order making the untenable argument that it cannot provide any such assistance to the extent that the target phone receives calls from a phone located in a foreign country or is otherwise used outside of the United States. *Cf. United States v. Cano-Flores*, 796 F.3d 83, 86-87 (D.C. Cir. 2015) (upholding wiretaps of cellular phones located in Mexico serviced by Nextel where the communications were first listened to by law enforcement within the issuing court's jurisdiction).

Moreover, the Wiretap Act is not *in personam* in the same way that the SCA is. A wiretap provisions only allow a court to order providers to ***assist*** law enforcement's investigative efforts that are authorized by the court. In contrast, the SCA directly grants authority to courts to require providers to produce certain information. This distinction matters. To the extent that the Wiretap Act grants courts *in personam* power to require providers to provide assistance, it follows that such assistance could require providers to take some action that occurs outside of the United States. For example, assume the government obtains a wiretap order that allows it to conduct a wiretap at a

facility located in the United States and requires the telecom provider to provide necessary assistance. Execution of the wiretap requires either some expertise from an employee that happens to work in a foreign office or some sort of hardware adapter that sits in that same office. The order requiring the provider to provide such assistance would require that provider to seek the foreign employee's expertise or send the necessary adapter to the domestic facility. There would be no basis for the provider to argue that the order is impermissible because it requires some activity that occurs abroad precisely because the court is exerting *in personam* power over it with respect to its assistance.

## III. Google Raises Unsupported And Unwarranted Concerns Regarding International Comity.

Prior to the *Microsoft* decision last year, providers like Google routinely produced information responsive to SCA warrants in their possession regardless of location. Ignoring that, as well as the multiples decisions concluding *Microsoft* was wrongly decided, Google argues returning to the status quo pre-*Microsoft* will spark international discord. *See, e.g.*, Google Mem. at 23 & n.8.

However, as set forth in its briefing below, the United States and at least 54 other countries have concluded, in connection with the Council of Europe's Convention on Cybercrime (the "Cybercrime Convention"), that compelling a person or entity located domestically to produce data that is in its control or custody, regardless of location, is a ***domestic exercise*** of power. *See generally* Memorandum of Law in Support of the Government's Motion for an Order Directing Google to Comply with a Warrant for Disclosure of Records at 13-17; *see also* Gov't Reply at 29-33. Indeed, as stated by the Supreme Court, the "presumption [against extraterritoriality] 'serves to protect against unintended

clashes between our laws and those of other nations which could result in international discord.'" *Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659, 1664 (2013) (citing *EEOC v. Arabian American Oil Co.*, 499 U.S. 244, 248 (1991)). Here, the Cybercrime Convention reflects agreement among the United States and 54 other countries that compelling a person or entity located domestically to produce data that is in its control or custody, regardless of location, is a domestic exercise of power.[15]

Google, however, notes the existence of certain "blocking statutes" enacted by "some governments [to] … combat the ability of foreign governments to regulate persons and data within their country." Google Mem. at 23 & n.8. It does not, however, claim any blocking statute would be applicable to the data called for here. *Id.* Indeed, it cannot make that claim because "Google cannot say with any certainty which foreign country's sovereignty would be implicated when Google accesses the content of communications in order to produce it in response to legal process" in part because it cannot "determine the location of the data" for all of its services. *EDPA Decision*, 232 F. Supp. 3d at 712, 723. Moreover, courts have routinely held that the existence of blocking statutes does not bar a court from ordering a party properly before it to disclose information in its control that is subject to such restrictions. *See Reinsurance Co. of Am.*, 902 F.2d at 1282 (noting that even where a blocking

[15] Judge Hammer also interpreted the Government's position here to be that the Cybercrime Convention "satisfy[ies] step one of *Morrison*." *See DNJ Decision*, 2017 WL 2985391, at *9. However, as set forth in the Government's briefing, "[t]he government does not argue that the ratification of the Cybercrime Convention expresses a clear intent that the SCA apply extraterritorially, instead, it argues that the Senate's ratification process, coupled with Congress's subsequent amendments to the SCA, express Congress's understanding that" the application of the SCA the Government seeks here is a "***domestic exercise*** of power." Gov't Reply at 30.

statute exposes a person to criminal sanctions in the foreign country if she produces information responsive to a U.S. court order, such statutes do not "automatically bar a domestic court from compelling production"); *Bank of Nova Scotia*, 691 F.2d at 1389-91 (compelling bank to respond to grand jury subpoena despite the existence of an applicable blocking statute).

Instead, Google refers to two amicus briefs filed in the *Microsoft* litigation. Google Mem. at 23 n.8. The first was filed by a single member of the European Parliament. The second is an amicus brief filed by Ireland. Contrary to Google's claim, the brief filed by Ireland does not at all suggest that Ireland's position was that compelling Microsoft to produce the data at issue would undermine its own authority. *See* Brief of Amicus Curiae Ireland, In the Matter of A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION at 3 (2d Cir. Dec. 23, 2014). In fact, Ireland's brief concluded that "in certain circumstances, an Irish court is prepared to order the disclosure by an Irish corporation of information in its possession, notwithstanding that the information is physically located in another jurisdiction…." *Id.* at 7. This is wholly consistent with the fact that many countries already assert even broader authority than what the SCA already provides. *See, e.g.*, Winston Maxwell & Christopher Wolf, A Global Reality: Governmental Access to Data in the Cloud, 2-3 (Hogan Lovells) (Updated 18 July 2012) ("Notably, ***every single country that we examined*** vests authority in the government to require a Cloud service provider to disclose customer data in certain situations, and in most instances this authority enables the government to access data physically stored outside the country's borders, provided there is some jurisdictional hook, such as the presence of a business within the country's borders" (examining laws of Australia, Belgium, Brazil, Canada, Colombia, Denmark, France, Ireland,

Mexico, Montenegro, Norway, Peru, Portugal, Serbia, Spain, and the United Kingdom)) (emphasis added).[16]

[16] http://www.cil.cnrs.fr/CIL/IMG/pdf/Hogan_Lovells_White_Paper_Government_Access_to_Cloud_Data_Paper_1_.pdf

## CONCLUSION

For the foregoing reasons, the government respectfully requests that this Court overrule Google's objections and affirm Magistrate Judge Hammer's order commanding Google to disclose all of the records and information responsive to the warrant that are within the possession, custody, or control of Google, regardless of whether such information is stored, held, or maintained inside or outside of the United States.

Dated: August 21, 2017

Respectfully submitted,

WILLIAM E. FITZPATRICK
Acting United States Attorney

/s/ L. Judson Welle

L. JUDSON WELLE
BRUCE P. KELLER
Assistant United States Attorneys

ANDREW S. PAK
Trial Attorney
Computer Crimes & Intellectual Property Section
United States Department of Justice

**CERTIFICATE OF SERVICE**

I hereby certify that true and correct copies of the Government's Memorandum of Law in response to Google Inc.'s Objections to Magistrate Judge's Order, dated August 21, 2017, were served via email upon the following counsel for Google, Inc.:

Jeffrey D. Vanacore, Esq.
JVanacore@perkinscoie.com
PERKINS COIE LLP
30 Rockefeller Plaza, 22nd Floor
New York, NY 10112-0085
Telephone: 212-262-6900
Facsimile: 212-977-1649

/s/
_____
L. Judson Welle
Assistant United States Attorney

Date: August 21, 2017